

# TOWARDS AN ASSESSMENT OF FAULT-TOLERANT DESIGN PRINCIPLES FOR SOFTWARE

Dave E. Eckhardt, Jr.  
NASA Langley Research Center

NASA  
Computer Science / Data Systems  
Technical Symposium

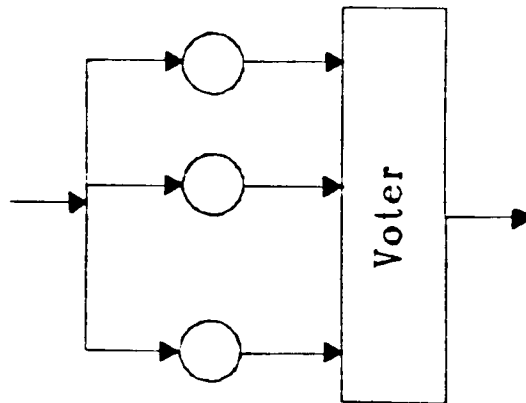
April 16-18, 1985

N87-29125

p. 20

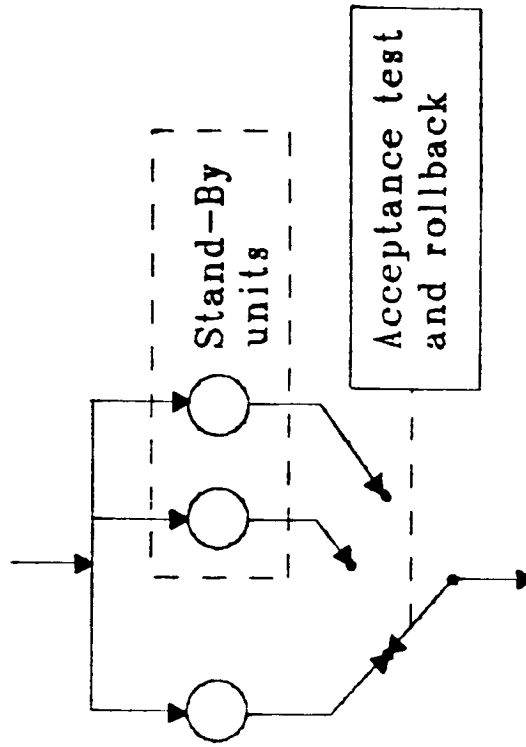
## FAULT-TOLERANT SOFTWARE

Dissimilar, redundant software structured to reduce the probability of system failure due to software faults. Techniques address error detection and isolation, system recovery, and continued service.



HARDWARE: N-Modular Redundancy

SOFTWARE: N-Version Programming



Stand-By Sparing

Recovery Block

# FAULT-TOLERANT SYSTEMS BRANCH: SOFTWARE RESEARCH SUPPORTED BY THE COMPUTER SCIENCE PROGRAM

## DESIGN:

- OPERATING SYSTEMS
  - Investigation of fault-tolerant software for SIFT operating system (Brunelle, NASA LaRC)
- SYSTEM THEORY
  - Integration of control system--theoretic FDI Techniques (Caglayan, Charles River Analytics)
- NEW TECHNOLOGY
  - Automatic generation of FDI software (Wild, ODU)

## RELIABILITY ASSESSMENT:

- EXPERIMENTAL
  - Investigation of independence assumption (Knight, UVA & Leveson, UCI)
  - Investigation of test procedures for multi-version software (McAllister, NC State)
- MODELS
  - Assessment of generic software reliability models (Migneault, NASA LaRC)
  - Development of basis for analysing strategy of software redundancy (Eckhardt, Lee, NASA LaRC)

## THE BASIS FOR FAULT-TOLERANT SOFTWARE

- Software faults are assumed to be "independent" so that errors will be randomly distributed among replicate codes.
- Currently, there are research efforts to analyse this fundamental assumption.

## HOWEVER

- Independence is not strictly needed for fault-tolerant software to be effective at reducing failure probability.
- It is a mathematically convenient assumption used to project the reliability of software fault-tolerant structures.

## ASSESSING FAULT-TOLERANT SOFTWARE

If software errors are not randomly distributed, what is the impact on reliability?

Current state of the art does not provide answers.

Consider:

- (1) Is an N-Version system of highly reliable components always more effective at reducing failure probability than a single version of software (on average)? If not, what causes this?
- (2) What are the effects of different intensities of coincident errors on software redundancy?
- (3) What is the effect of increasing N? Is there a limit to the effectiveness of software redundancy? Might an optimum value of N exist?
- (4) Does the independence model provide a valid estimate of the failure probability of an N-Version system?
- (5) Under what condition does independence hold?

## GOAL OF CURRENT RESEARCH

### Assess strategy of software redundancy

- population concepts
- sampling, sample size
- inference

### AS OPPOSED TO:

### Assessing an instance of fault-tolerance

- decide number of versions
- develop
- measure

# QUANTITIES DESCRIBING COINCIDENT ERRORS MODEL

INPUT SPACE

	$\{$	$x_1$	$x_2$	$x_3$	$\dots$	$x_k$	$\}$	
$C_1$		0	1	0	$\dots$	0		$v_1(x)$
$C_2$		1	0	0	$\dots$	1		
$\vdots$								
$C_l$		0	1	0	$\dots$	0		
$\vdots$								

$\theta(x_1)$

COMPONENT  
POPULATION

CONDITIONAL FAILURE PROBABILITY

$$Q(F) = \int v_1(x) \, dQ$$

$$= \Pr\{C_l \text{ fails}\}$$

$Q$  = USAGE DISTRIBUTION

AVERAGE FAILURE PROBABILITY

$$E[\int v(x) \, dQ] = \int \theta(x) \, dQ$$

INTENSITY FUNCTION

$$\theta(x) = \Pr\{v(x) = 1\}$$

$$E[v(x)] = \theta(x)$$

INTENSITY DISTRIBUTION

$$G(y) = \int \{x : \theta(x) \leq y\} \, dQ$$

# N-VERSION WITH MAJORITY VOTE

	IID INPUT			
RANDOM SAMPLE	$v_1(\mathbf{x})$	0	0	1 ...
	$v_2(\mathbf{x})$	0	1	0 ...
	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	$v_N(\mathbf{x})$	0	0	0 ...

## SCORE FUNCTION

$$v(\mathbf{x}) = \sum_{l=1}^N \sum_{\substack{\text{all} \\ \text{permutations, } i}} v_{l(1)}(\mathbf{x}) \dots v_{l(l)}(\mathbf{x}) [ 1 - v_{l(l+1)}(\mathbf{x}) ] \dots [ 1 - v_{l(N)}(\mathbf{x}) ]$$

$$P_N = E[ \int v(\mathbf{x}) \, d\mathbf{Q} ]$$



# COINCIDENT ERRORS MODEL

Under the conditions that:

- (1) components are selected from a random sample
- (2) inputs are selected from a common distribution

$$p_N = \int \sum_{t=m}^N \binom{N}{t} \theta(x)^t [1 - \theta(x)]^{N-t} dQ$$

$\theta(x)$  = Intensity Function

$Q$  = Usage Distribution

$$= \int h(y;N) dG$$

$$h(y;N) = \sum_{t=m}^N \binom{N}{t} y^t [1-y]^{N-t}$$

$$G(y) = \int_{\{x : \theta(x) \leq y\}} dQ = \text{Intensity Distribution}$$

# A DISCRETE INTENSITY DISTRIBUTION

Suppose  $\theta(x) = \theta_i$  for  $x \in A_i$

Where  $A_1, A_2, \dots, A_r$  is a partition of  $\Omega$

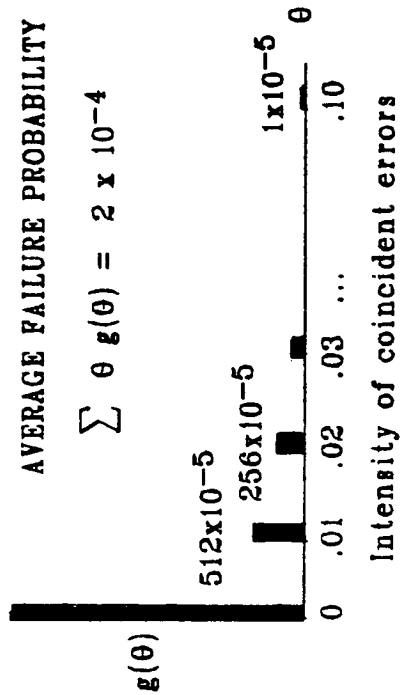
Indexing so that

$$0 = \theta_1 < \theta_2 < \dots < \theta_r < 1$$

$$G(y) = \sum_{\{i : \theta_i \leq y\}} Q(A_i) \quad -\infty \leq y \leq \infty$$

e.g

.98977



(e.g. on .001% of inputs, expect 10% of population to produce error)

## EFFECTS OF COINCIDENT ERRORS

Under what condition does independence hold?

Under the assumption of a constant intensity the Coincident Errors Model implies the Independent Errors Model.

This constant is the average component failure probability ( also the mean of the Intensity Distribution).

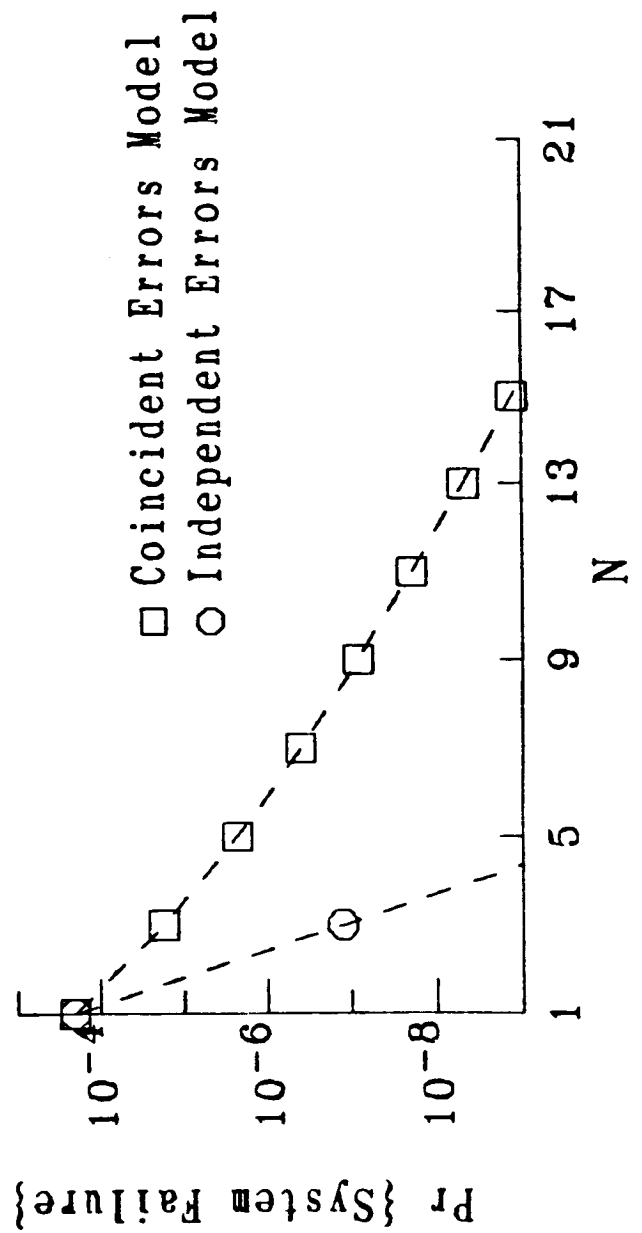
$$P = \int \theta(x) \, dQ = \int y \, dG(y).$$

# EFFECTS OF COINCIDENT ERRORS

Does the Independence Model give a valid estimate of failure probability?

e.g

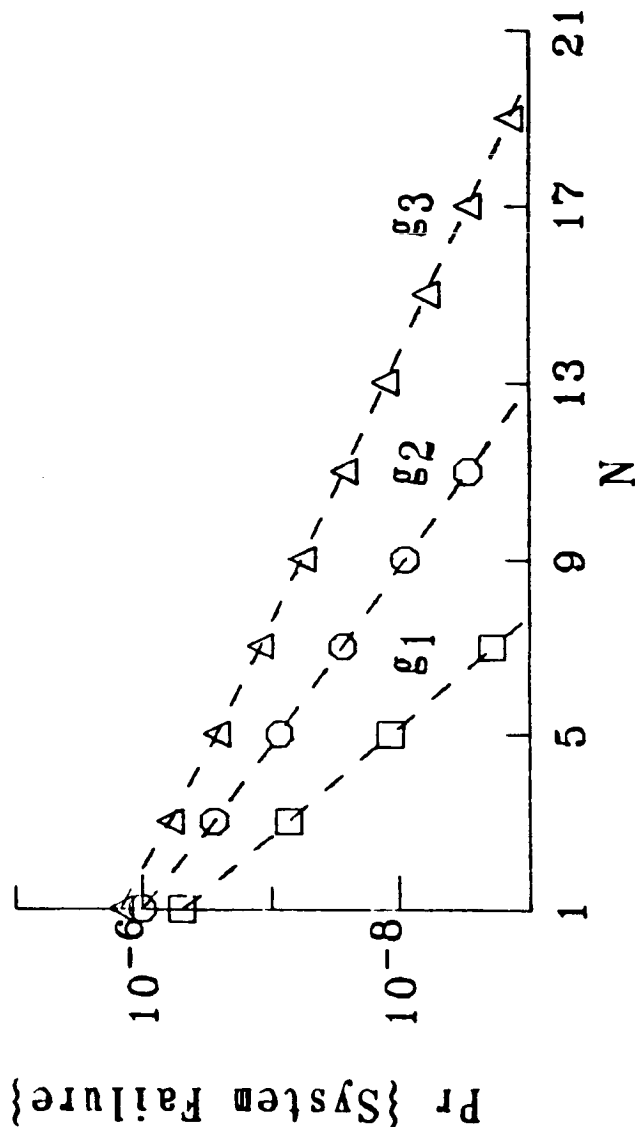
$\theta$	$g(\theta)$
0	.98977
.01	.00512
.02	.00256
$\vdots$	$\vdots$
.10	.00001



# EFFECTS OF COINCIDENT ERRORS

What is the effect of shifting intensity  
mass probability to the right?  
e.g.

$\theta$	$g_1(\theta)$	$g_2(\theta)$	$g_3(\theta)$
0	.99999	.99999	.99999
.05	.00001		
.10		.00001	
.15			.00001

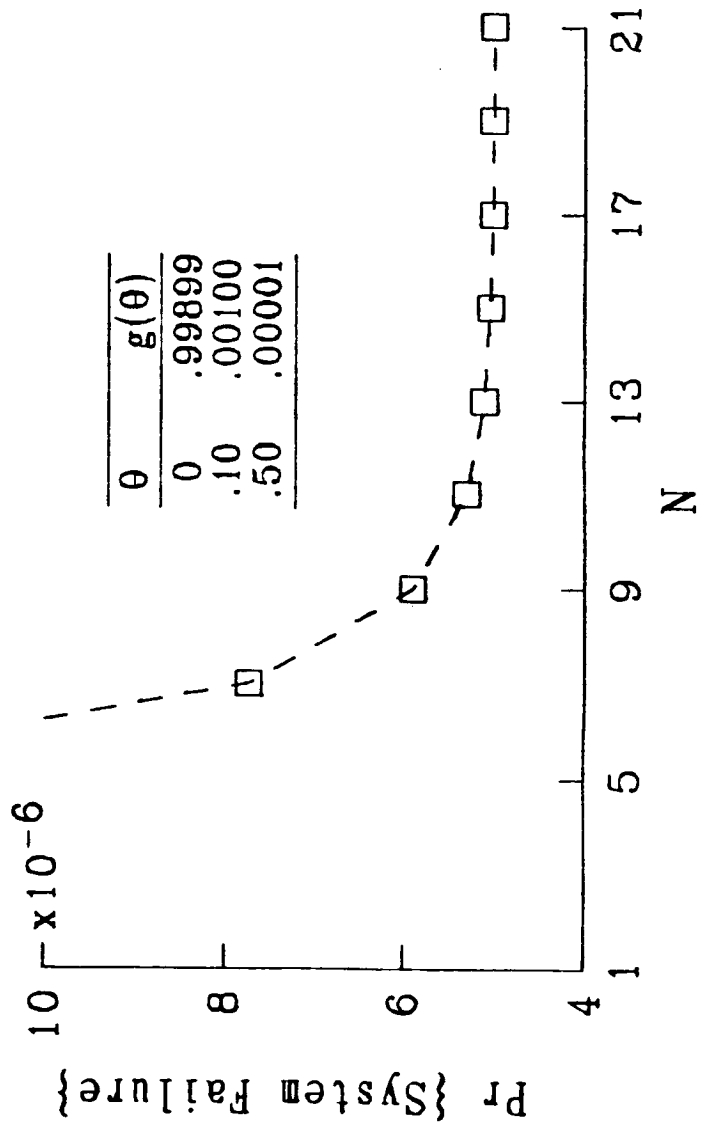


# EFFECTS OF COINCIDENT ERRORS

Is there a limit on the effectiveness of redundancy?

Effectiveness limited by mass distributed  
along interval  $.5 \leq \theta \leq 1$

$$\lim_{N \rightarrow \infty} P_N = .5 \left[ G(.5^+) - G(.5^-) \right] + \int_{.5^+}^1 dG(\theta)$$



# EFFECTS OF COINCIDENT ERRORS

Under what condition is an N-Version strategy better than a single version choosen at random?

We say an N-Version strategy is better if  $P_N < P$

Where

$$P_N = \int \sum_{l=m}^N \binom{N}{l} \theta(x)^l (1 - \theta(x))^{N-l} dQ$$

$$= \int h(y;N) dG(y)$$

and

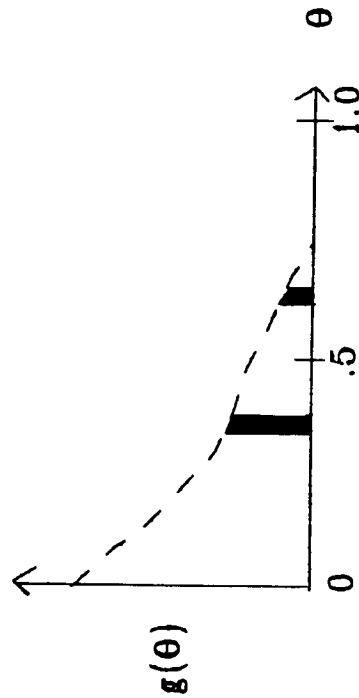
$$P = \int \theta(x) dQ = \int y dG(y)$$

# EFFECTS OF COINCIDENT ERRORS

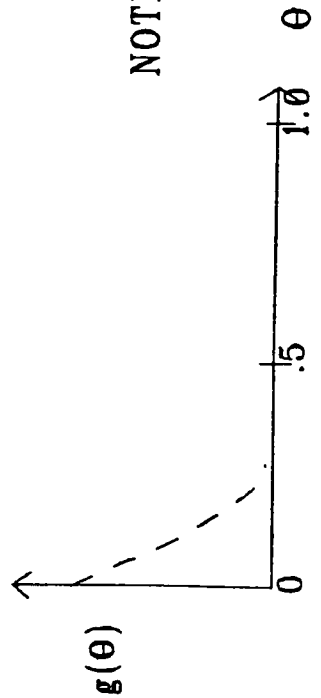
If the asymmetry condition,

$$\int_{(y, y+\Delta]} dG \geq \int_{[1-y-\Delta, 1-y)} dG,$$

holds for  $y, y+\Delta < .5$ , then  $P_N < P$ .



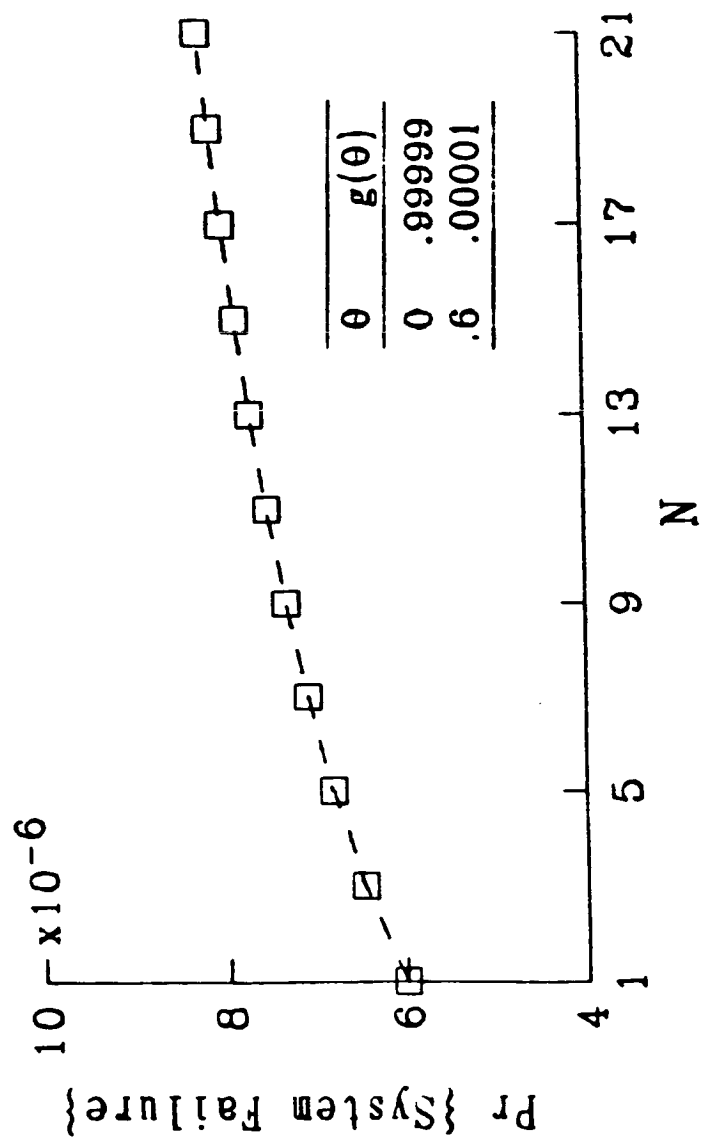
In particular, the asymmetry condition holds whenever the Intensity Distribution is limited above by .5.



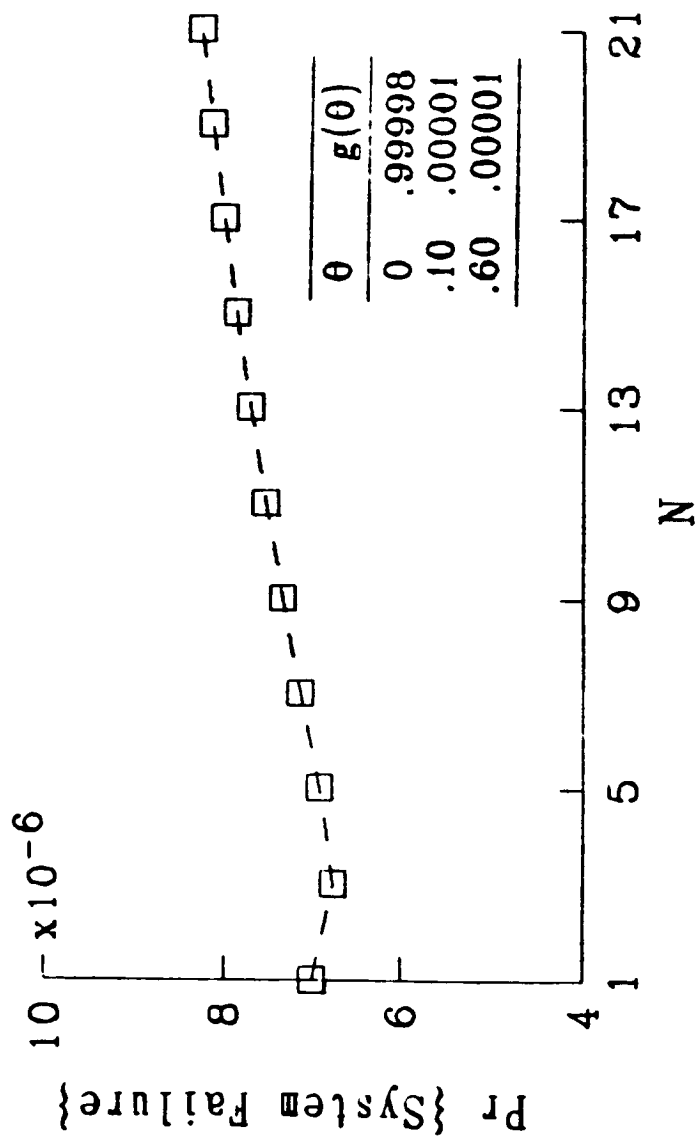
NOTE:  $P < .5 \not\Rightarrow P_N < P$



# EFFECTS OF COINCIDENT ERRORS



# EFFECTS OF COINCIDENT ERRORS

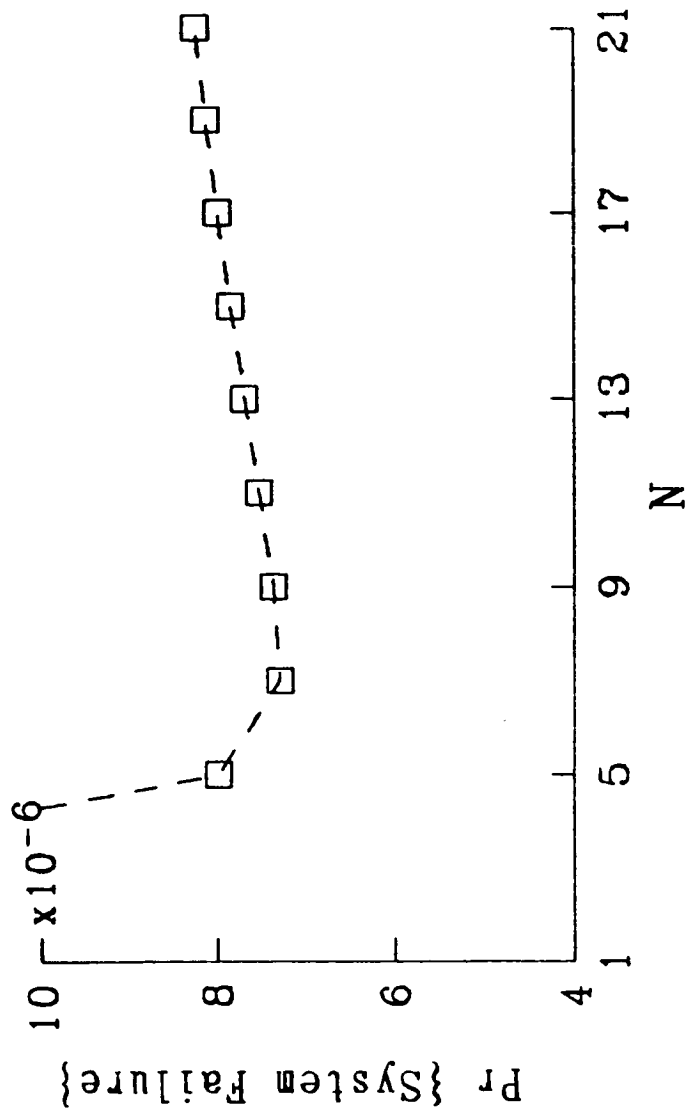


# EFFECTS OF COINCIDENT ERRORS

Might an optimum value of  $N$  exist?

A necessary condition for system degradation in the limit is a violation of asymmetry condition.  
e.g.

$\theta$	$g(\theta)$	Note: asymmetry condition not necessary for $P_N < P$
0	.99899	
.05	.00100	
.60	.00001	



## RESULTS

- Provides a probabilistic framework for assessing strategy of redundant software.
- Provides foundation for experimental study of coincident errors.
- Permits an analytical study to increase understanding of impact of coincident errors.